



XML Broadly Connecting Canadian IT managers through Career, Industry, and Technology insight

**This Blog**

About

Email

| Feb | March 2006 |    |    | Apr |    |    |
|-----|------------|----|----|-----|----|----|
| S   | M          | T  | W  | T   | F  | S  |
| 26  | 27         | 28 | 1  | 2   | 3  | 4  |
| 5   | 6          | 7  | 8  | 9   | 10 | 11 |
| 12  | 13         | 14 | 15 | 16  | 17 | 18 |
| 19  | 20         | 21 | 22 | 23  | 24 | 25 |
| 26  | 27         | 28 | 29 | 30  | 31 | 1  |
| 2   | 3          | 4  | 5  | 6   | 7  | 8  |

**Search**
 **Go**
**Archives**

March 2006 (8)

February 2006 (41)

January 2006 (26)

December 2005 (26)

November 2005 (8)

October 2005 (6)

September 2005 (2)

August 2005 (7)

**News**

These postings are provided "AS IS" with no warranties, and confers no rights. You assume all risk for your use.

» Blogs that link here

**Resident Bloggers**

Stephen Ibaraki

Technology Journalist I.S.P., DF/NPA, CNP

John Oxley

Director IT Pro Evangelism  
Microsoft Canada

Barnaby Jeans

IT Pro Advisor  
Microsoft Canada**Guest Bloggers**

Val Matison

CIO

Info3

**GOT A  
QUESTION?****Best Practices for Performing a Security Audit from Laura Chappell**

I was talking with [Laura Chappell](#) about useful security tips since she "lives and breathes" security. As a bit of background, last year, she received the international Award for Professionalism founded by the NPA and given out at the Interop Conference in Vegas. Some of you may have caught her packed sessions at Microsoft TechEd conferences or HP Enterprise Symposiums. I know from my talks with some of you, you are familiar with her "[Internet Safety for Kids Project](#)" which she founded together with the "[Protocol Analysis Institute](#)."

Anyways, I asked her about the best ways to perform a security vulnerability audit on your network and she provided this list:

\*\*\*

Well, Stephen, there are so many ways to go about this so I'll just start spewing out options:

1. Identify assets (risk assessment)
2. Prioritize the audit focus (separate the task into smaller chunks)
3. Differentiate between intrusive and non-intrusive audit procedures
4. Map the network from outside and inside the firewall
5. Audit server and client software and hardware
6. Examine software/hardware audit results against an 'acceptable' list
7. Examine log files and log file usage
8. Audit routers, firewalls and critical infrastructure devices
9. Verify system and user configurations
10. Audit application traffic for cleartext data transfer or unusual dependencies
11. Audit all network access points (dial-in, wireless, tunnels, partner/consultant links)
12. Audit security training information for users, management, consultants
13. Check against industry-known vulnerabilities
14. Audit antivirus and anti-spyware capabilities and status
15. Audit patch and fix levels for hosts and servers (multiple OS types too)

\*\*\*

Laura shares more of her best practices and provides her viewpoint on security in an upcoming interview. Look for it here...

Thank you,  
Stephen Ibaraki

Published Thursday, March 02, 2006 8:56 AM by [cdnltmgr](#)  
Filed Under: [Industry Perspectives](#), [Stephen Ibaraki](#)

**Comment Notification**

If you would like to receive an email when updates are made to this post, please register [here](#)

You can also stay up to date using your favorite aggregator by subscribing to the [CommentRss Feed](#)

**Comments****# Interesting Finds**

Friday, March 03, 2006 8:18 AM by [Jason Haley](#)

**What do you think?**Title *(required)*

Name *required*


Your URL

Comments *(required)*

**Navigation**

- [Home](#)
- [Photos](#)

**Post Categories**

- [Adam Cole \(2\)](#)
- [CC Blogged Down \(4\)](#)
- [Events \(6\)](#)
- [Guest Bloggers \(12\)](#)
- [Industry Perspectives \(12\)](#)
- [Interviews \(5\)](#)
- [Mitch Tulloch \(2\)](#)
- [MS News \(10\)](#)
- [Partners \(1\)](#)
- [Stephen Ibaraki \(25\)](#)
- [Training \(3\)](#)
- [Val Matison \(3\)](#)

Remember Me?